Amendments to the Claims: This listing of claims will replace all prior versions, and listings, of claims in the application

Listing of Claims:

1. (Currently Amended) A method for performing modular division operations used in a cryptographic process over a finite field F_U defined for a prime number U to generate a cryptographic key, in which cryptographic process ~~values are~~at least one value is divided by an integer divisor V modulo U, the method comprising the steps of calculating an arithmetic inverse of V modulo U using an extended greatest common divisor (GCD) method which includes a plurality of reduction steps and a plurality of inverse calculations, including the steps of:

assigning U and V as initial values to respective temporary variables U3 and V3 which are used to calculate the GCD of U and V;

assigning initial values to respective temporary variables U2 and V2 which are used to calculate an arithmetic inverse of V modulo U;

determining whether U3 has a number, N, of zero-valued least significant bits (LSBs), where N is an integer greater than two, and if N is greater than two, ~~testing a condition and, if the condition tests true,~~

combining multiple ones of the plurality of reduction steps for calculating the GCD; and

combining multiple ones of the plurality of inversion calculations; and

if N is not greater than 2, ~~the condition tests false,~~

performing a single one of the reduction steps; and

performing a single one of the inverse calculation steps;

returning, as a result of the plurality of reduction steps and the plurality of inverse calculations, the arithmetic inverse of V; and

as a part of the cryptographic process, multiplying the at least one value by the returned arithmetic inverse in place of the integer division to produce the cryptographic key.

2. (Currently Amended) A method according to claim 1, wherein: the extended GCD algorithm is a binary GCD algorithm;

PAGE 17/31 * RCVD AT 11/28/2005 3:32:29 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:6104070701 * DURATION (mm-ss):07-56

~~the step of testing the condition includes the step of determining if U3 has a number, N, of zero-valued least significant bits (LSBs), where N is an integer greater than one;~~

the step of combining multiple ones of the plurality of reduction steps includes shifting the value in U3 by N bit positions to less significant bit positions; and

the step of combining multiple ones of the plurality of inversion calculations includes the steps of:

retrieving a value to be combined with V2 from a look-up table responsive to the value of N;

combining the retrieved value from V2 to obtain a combined value in V2; and

shifting the combined value in V2 by N bit positions to less significant bit positions.

3. (Original) A method according to claim 2, wherein the look-up table includes a plurality of multiples of U.

4. (Original) A method according to claim 3, wherein the step of retrieving the value to be combined with V2 from a look-up table includes the steps of:

indexing a first further look-up table responsive to two of the LSBs of V2 if N equals 2 to obtain an index value;

indexing a second further look-up table responsive to three of the LSBs of V2 if N is greater than 2 to obtain the index value; and

indexing the look-up table by the index value.

5. (Currently Amended) A method according to claim ~~1~~6, wherein:

the extended GCD algorithm is a left-shift binary GCD algorithm; and

the steps of combining multiple ones of the plurality of reduction steps and combining multiple ones of the plurality of inversion calculations includes the step of performing a reduction step according to a Lehmer GCD method.

PAGE 18/31 * RCVD AT 11/28/2005 3:32:29 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:6104070701 * DURATION (mm-ss):07-56

6. (Currently Amended) A method ~~according to claim 5, wherein,~~ for performing modular division operations used in a cryptographic process over a finite field F_U defined for a prime number U to generate a cryptographic key, in which cryptographic process, at least one value is divided by an integer divisor V modulo U, the method comprising the steps of calculating an arithmetic inverse of V modulo U using an extended greatest common divisor (GCD) method which includes a plurality of reduction steps and a plurality of inverse calculations, including the steps of

assigning U and V as initial values to respective temporary variables U3 and V3 which are used to calculate the GCD of U and V;

assigning initial values to respective temporary variables U2 and V2 which are used to calculate an arithmetic inverse of V modulo U;

~~testing the condition includes the step of~~ determining ~~if~~whether a bit position of a most significant bit (MSB) of the value in U3 differs by less than a predetermined number from a bit position of an MSB of the value in V3, and if the bit position of the MSB of the value in U3 differs by less than the predetermined number from the bit position of the MSB of the value in V3,

combining multiple ones of the plurality of reduction steps for calculating the GCD; and

combining multiple ones of the plurality of inversion calculations; and

if the bit position of the MSB of the value in the U3 does not differ by less than the predetermined number from the bit position of the MSB of the value in the V3,

performing a single one of the reduction steps; and

performing a single one of the inverse calculation steps;

returning, as a result of the plurality of reduction steps and the plurality of inverse calculations, the arithmetic inverse of V; and

as a part of the cryptographic process, multiplying the at least one value by the returned arithmetic inverse in place of the integer division to produce the cryptographic key.

PAGE 19/31 * RCVD AT 11/28/2005 3:32:29 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:6104070701 * DURATION (mm-ss):07-56

7. (Currently Amended) A computer readable carrier including computer program instructions that cause a computer to perform modular division operations over a finite field F_U ~~that~~ defined for a prime number U and used in a cryptographic process in which ~~values are~~ at least one value is divided by an integer divisor V modulo U to generate a cryptographic key, the method comprising the steps of calculating an arithmetic inverse of V modulo U using an extended greatest common divisor (GCD) method which includes a plurality of reduction steps and a plurality of inverse calculations, including the steps of:

assigning U and V as initial values to respective temporary variables U3 and V3 which are used to calculate the GCD of U and V;

assigning initial values to respective temporary variables U2 and V2 which are used to calculate an arithmetic inverse of V modulo U;

determining whether U3 has a number, N, of zero-valued least significant bits (LSBs), where N is an integer greater than two, and if N is greater than two, ~~testing a condition and, if the condition tests true,~~

combining multiple ones of the plurality of reduction steps for calculating the GCD; and

combining multiple ones of the plurality of inversion calculations; and

if N is not greater than two, ~~the condition tests false,~~

performing a single one of the reduction steps; and

performing a single one of the inverse calculation steps;

returning, as a result of the plurality of reduction steps and the plurality of inverse calculations, the arithmetic inverse of V; and

as a part of the cryptographic process, multiplying the at least one value by the returned arithmetic inverse in place of the integer division to produce the cryptographic key.

PAGE 20/31 * RCVD AT 11/28/2005 3:32:29 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:6104070701 * DURATION (mm-ss):07-56

8. (Currently Amended) A computer readable carrier according to claim 7, wherein:

the extended GCD algorithm is a binary GCD algorithm~~ and the computer program instructions which implement the step of testing the condition cause the computer to perform the step of determining if U3 has a number, N, of zero-valued least-significant bits (LSBs), where N is an integer greater than one~~;

the computer program instructions which implement the step of combining multiple ones of the plurality of reduction steps cause the computer to perform the step of shifting the value in U3 by N bit positions to less significant bit positions; and

the computer program instructions which implement the step of combining multiple ones of the plurality of inversion calculations cause the computer to perform the steps of:

retrieving a value to be combined with V2 from a look-up table responsive to the value of N;

combining the retrieved value from V2 to obtain a combined value in V2; and

shifting the combined value in V2 by N bit positions to less significant bit positions.

9. (Original) A computer readable carrier according to claim 8, wherein the look-up table includes a plurality of multiples of U.

10. (Original) A computer readable carrier according to claim 9, wherein the computer program instructions that implement the step of retrieving the value to be combined with V2 from a look-up table cause the computer to perform the steps of:

indexing a first further look-up table responsive to two of the LSBs of V2 if N equals 2 to obtain an index value;

PAGE 21/31 * RCVD AT 11/28/2005 3:32:29 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:6104070701 * DURATION (mm-ss):07-56

indexing a second further look-up table responsive to three of the LSBs of V2 if N is greater than 2 to obtain the index value; and

indexing the look-up table by the index value.

11. (Currently Amended) A computer readable carrier according to claim ~~7~~12, wherein the extended GCD algorithm is a left-shift binary GCD algorithm and the computer program instructions that cause the computer to perform the steps of combining multiple ones of the plurality of reduction steps and combining multiple ones of the plurality of inversion calculations includes the step of performing a reduction step according to a Lehmer GCD method.

12. (Currently Amended) A computer readable ~~medium according to claim 11, wherein,~~carrier including computer program instructions that cause a computer to perform modular division operations over a finite field F_U that defined for a prime number U and used in a cryptographic process in which at least one value is divided by an integer divisor V modulo U to generate a cryptographic key, the method comprising the steps of calculating an arithmetic inverse of V modulo U using an extended greatest common divisor (GCD) method which includes a plurality of reduction steps and a plurality of inverse calculations, including the steps of:

assigning U and V as initial values to respective temporary variables U3 and V3 which are used to calculate the GCD of U and V;

assigning initial values to respective temporary variables U2 and V2 which are used to calculate an arithmetic inverse of V modulo U;

~~testing the condition includes the step of~~ determining ~~if~~whether a bit position of a most significant bit (MSB) of the value in U3 differs by less than a predetermined number from a bit position of an MSB of the value in V3, and if the bit position of the MSB of the value in U3 differs by less than the predetermined number from the bit position of the MSB of the value in V3,

combining multiple ones of the plurality of reduction steps for calculating the GCD; and

PAGE 22/31 * RCVD AT 11/28/2005 3:32:29 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:6104070701 * DURATION (mm-ss):07-56

combining multiple ones of the plurality of inversion calculations; and

if the bit position of the MSB of the value in the U3 does not differ by less than the predetermined number from the bit position of the MSB of the value in the V3,

performing a single one of the reduction steps; and

performing a single one of the inverse calculation steps;

returning, as a result of the plurality of reduction steps and the plurality of inverse calculations, the arithmetic inverse of V; and

as a part of the cryptographic process, multiplying the at least one value by the returned arithmetic inverse in place of the integer division to produce the cryptographic key.

13. (Currently Amended) Cryptographic apparatus which performs division operations over a finite field F_U defined for a prime number U, in which ~~values are~~ at least one value is divided by an integer divisor V modulo U to generate a cryptographic key, the apparatus calculating an arithmetic inverse of V modulo U using an extended greatest common divisor (GCD) algorithm which includes a plurality of reduction steps and a plurality of inverse calculations, the apparatus comprising:

means for assigning U and V as initial values to respective temporary variables U3 and V3 which are used to calculate the GCD of U and V;

means for assigning initial values to respective temporary variables U2 and V2 which are used to calculate an arithmetic inverse of V modulo U;

means for ~~testing a condition~~determining whether U3 has a number, N, of zero-valued least significant bits (LSBs), where N is an integer greater than two; and

means for combining multiple ones of the plurality of reduction steps and multiple ones of the inverse calculations if ~~the condition test true;~~ N is greater than two;

means for returning, as a result of the plurality of reduction steps and the plurality of inverse calculations, the arithmetic inverse of V; and

as a part of the cryptographic process, means for multiplying the at least one value by the returned arithmetic inverse in place of the integer division to produce the cryptographic key.

14. (Currently Amended) Cryptographic apparatus according to claim 13, wherein:

the extended GCD algorithm is a binary GCD algorithm;

~~the means for testing the condition includes means for determining if U3 has a number, N, of zero valued least significant bits (LSBs), where N is an integer greater than one;~~

the means for combining multiple ones of the plurality of reduction steps includes means for shifting the value in U3 by N bit positions to less significant bit positions; and

the means for combining multiple ones of the plurality of inversion calculations includes:

means for retrieving a value to be combined with V2 from a look-up table responsive to the value of N;

means for combining the retrieved value from V2 to obtain a combined value in V2; and

means for shifting the combined value in V2 by N bit positions to less significant bit positions.

15. (Original) Apparatus according to claim 14, wherein the look-up table includes a plurality of multiples of U.

16. (Original) Apparatus according to claim 15, wherein:

PAGE 24/31 * RCVD AT 11/28/2005 3:32:29 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:6104070701 * DURATION (mm-ss):07-56

the means for retrieving the value to be combined with V2 from a look-up table includes:

means for indexing a first further look-up table responsive to two of the LSBs of V2 if N equals 2 to obtain an index value;

means for indexing a second further look-up table responsive to three of the LSBs of V2 if N is greater than 2 to obtain the index value; and

means for indexing the look-up table by the index value.

17. (Currently Amended) Apparatus according to claim ~~13~~18, wherein:

the extended GCD algorithm is a left-shift binary GCD algorithm; and

the means for combining multiple ones of the plurality of reduction steps and multiple ones of the plurality of inversion calculations includes means for performing a reduction step according to a Lehmer GCD method.

18. (Currently Amended) Cryptographic apparatus which performs division operations over a finite field F_U defined for a prime number U, in which at least one value is divided by an integer divisor V modulo U to generate a cryptographic key, the apparatus calculating an arithmetic inverse of V modulo U using an extended greatest common divisor (GCD) algorithm which includes a plurality of reduction steps and a plurality of inverse calculations, the apparatus comprising:~~Apparatus according to claim 17 wherein, the means for testing the condition includes~~

means for assigning U and V as initial values to respective temporary variables U3 and V3 which are used to calculate the GCD of U and V;

means for assigning initial values to respective temporary variables U2 and V2 which are used to calculate an arithmetic inverse of V modulo U;

means for determining ~~if~~whether a bit position of a most significant bit (MSB) of the value in U3 differs by less than a predetermined number from a bit position of an MSB of the value in V3[[.]]; and

means for combining multiple ones of the plurality of reduction steps and multiple ones of the inverse calculations if the bit position of the MSB of the value in U3 differs by less than the predetermined number from the bit position of the MSB of the value in V3.

PAGE 26/31 * RCVD AT 11/28/2005 3:32:29 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/24 * DNIS:2738300 * CSID:6104070701 * DURATION (mm-ss):07-56